Title (en)

PUBLIC/PRIVATE KEY SYSTEM WITH INCREASED SECURITY

Title (de)

ÖFFENTLICHES/PRIVATES SCHLÜSSELSYSTEM MIT ERHÖHTER SICHERHEIT

Title (fr)

SYSTÈME DE CLÉ PUBLIQUE/PRIVÉE À SÉCURITÉ ACCRUE

Publication

EP 4082153 A1 20221102 (EN)

Application

EP 20833923 A 20201224

Priority

- EP 19219637 A 20191224
- EP 20167254 A 20200331
- EP 2020087868 W 20201224

Abstract (en)

[origin: EP3843321A1] Some embodiments are directed to a second cryptographic device (20) and a first cryptographic device (10). The first and second cryptographic devices may be configured to transfer a key seed. The key seed may be protected using a public key from one party and a private key from the other party. For example, a public key may be obtained from a private key through a noisy multiplication. At least one of the first and second cryptographic device may validate an obtained public key, e.g., to avoid leakage of the key seed or of a private key.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP US)

H04L 9/0841 (2013.01 - EP US); **H04L 9/14** (2013.01 - US); **H04L 9/3093** (2013.01 - EP US)

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

Designated validation state (EPC)

KH MA MD TN

DOCDB simple family (publication)

EP 3843321 A1 20210630; CN 114902605 A 20220812; EP 3843320 A1 20210630; EP 4082153 A1 20221102; EP 4082153 B1 20230816; US 11917063 B2 20240227; US 2023052293 A1 20230216; WO 2021130366 A1 20210701

DOCDB simple family (application)

EP 20167254 A 20200331; CN 202080090387 A 20201224; EP 19219637 A 20191224; EP 2020087868 W 20201224; EP 20833923 A 20201224; US 202017786573 A 20201224